Quantum Cloning of Mixed States in Symmetric Subspace

Heng Fan[1] *

[1] *ERATO Quantum Computation and Information Project, JST.*
Hongo White Building, 5-28-3 Hongo, Bunkyo-ku, Tokyo 113-0033, Japan.

Abstract. Quantum cloning machine for arbitrary mixed states in symmetric subspace is proposed. This quantum cloning machine can be used to copy part of the output state of another quantum cloning machine and is useful in quantum computation and quantum information. The shrinking factor of this quantum cloning achieves the well-known upper bound. When the input is identical pure states, two different fidelities of this cloning machine are optimal.

Keywords: No-cloning theorem, quantum cloning machine, fidelity.

A simple but practical quantum cloning task: A quantum state cannot be cloned exactly because of the no-cloning theorem[1]. However, quantum cloning approximately (or probabilisticaly) is necessary in quantum computation and quantum information[2]. Suppose we have the following task: we have a pure unknown quantum state in 2-level system (qubit) $|\Psi\rangle$. We need one copy of this quantum state to perform one quantum computation. But we do not need it to be exactly the original one. A copy of $|\Psi\rangle$ with fidelity of at least $7/9$ can give a reliable result. And also we need another 3 identical quantum states each with the fidelity of at least $79/108$ to perform another reliable quantum computation. If the fidelities of the quantum states are less than the demanding fidelities, the quantum computation will not be reliable any more. This is certainly a simple and rather practical quantum cloning task. However, we still cannot reach this simple goal by the present available optimal quantum cloning machines.

Let's next analyze why the present available quantum cloning machines fail to do this work. 1, First we try to use the 1 to 4 optimal quantum cloning machine proposed by Gisin and Massar[3] to do this work. By this cloning machine, we can copy $|\Psi\rangle$ to 4 identical quantum states each with fidelity $3/4$ which is larger than $79/108$ but less than $7/9$. That means we can obtain a reliable result in the second quantum computation but we cannot have a reliable result in the first quantum computation. 2, We may use first the 1 to 2 cloning machine which is proposed by Buzek and Hillery[4, 5]. With one output state doing the first quantum computation, then we use another quantum state as input and use the 1 to 3 Gisin-Massar cloning machine to create another 3 identical quantum states. One can find the quantum state of the first cloning machine can achieve the fidelity $5/6$ which is better than the demanding fidelity $7/9$. However, the 3 identical quantum states can only achieve the fidelity $37/54$ which is lower than the demanding fidelity. So, we cannot finish our task by using this method. 3, One is perhaps tempted to use Cerf's asymmetric quantum cloning machine[6] to do this work. The advantage of using Cerf's asymmetric cloning machine is that we can let one quantum state achieve the fidelity $7/9$ while another one still has the optimal fidelty since this cloning machine achieve the bound of the no-cloning theorem proposed by Cerf, see appendix for the detail. Then we use the Gisin-Massar 1 to 3 cloning machine to create another 3 identical quantum states. By calculation we can find if one quantum state has fidelity $7/9$, the optimal fidelity achieved by another quantum state is $11 + 2\sqrt{6}/18 \approx 0.88$. However, we need it at least $11/12 \approx 0.92$ to create reliable 3 identical quantum states by using Gisin-Massar cloning machine. So, we still cannot achieve our aim.

The quantum cloning machine which can accomplish the previous quantum cloning task: Is this task in principal cannot be accomplished since no-cloning theorem? By simple calculation we can show that this goal in principal can be achieved. The following is one method. We can first use the Gisin-Massar 1 to 3 cloning machine. And after this quantum cloning, we can use one quantum state which has fidelity $7/9$ to perform the first quantum computation which will give the reliable result. The remaining quantum state is a two qubits mixed state in symmetric subspace. The theory of Bruss, Ekert and Macchiavello (BEM) [7] shows that the optimal shrinking factor, which has a simple relation with fidelity for pure state, of 2 to 3 cloning machine can achieve $5/6$. So, we can obtain 3 quantum states each with fidelity $79/108$ which will also give a reliable result in the second quantum computation. Thus both two quantum computations will give reliable results. The Gisin-Massar cloning machine can only copy 2 *identical pure* states to 3 copies. The problem is that here the input state of 2 qubits is a mixed states in symmetric space which cannot be copied by the available cloning machines. So we must construct a 2 to 3 optimal cloning machine which can use a mixed state in symmetric subspace as input.

One can imagine that a lot of other similar problems exist in the quantum computation. In this paper we will first present explicitly the quantum cloning machine which can accomplish the above mentioned task. And further some more complicated tasks similar to the above one can also be accomplished. Our result is actually rather general. We will present the optimal quantum cloning machine which can use arbitrary d-level mixed states in symmetric subspace as input. And the cloning machine is optimal since it achieves the upper bound of the shrinking factor [7, 8, 9]. The cloning machine pre-

*fan@qci.jst.go.jp

sented in this paper can also be used directly to analyze the security of quantum key distribution when all $d+1$ mutually unbiased states are used which provides the most secure protocol in d-level quantum system, here d is assumed to be prime number in this quantum key distribution protocol.

Let's study the quantum cloning task presented above. We assume the available unknow quantum state is expressed as $|\Psi\rangle = \alpha|\uparrow\rangle + \beta|\downarrow\rangle$ with $|\alpha|^2 + |\beta|^2 = 1$. First we use Gisin-Massar 1 to 3 cloning machine[3] which will create 3 copies of $|\Psi\rangle$ approximately. One output state is $\rho_{red.} = 5/9|\Psi\rangle\langle\Psi| + 2/9 \cdot I$, where I is the identity. The fidelity of $\rho_{red.}$ with the original quantum state $|\Psi\rangle$ is 7/9 which achieve the threshold to give a reliable result in the first quantum computation. The remaining 2 qubits state which is obtained after tracing out 1 qubit used for the first quantum computation from the output state takes the form

$$\begin{aligned}\rho^{(2)}_{red.} &= x_0|2\uparrow\rangle\langle 2\uparrow| + x_1|2\uparrow\rangle\langle\uparrow,\downarrow| \\ &+ x_1^*|\uparrow,\downarrow\rangle\langle 2\uparrow| + \frac{1}{3}|\uparrow,\downarrow\rangle\langle\uparrow,\downarrow| + x_1|\uparrow,\downarrow\rangle\langle 2\downarrow| \\ &+ x_1^*|2\downarrow\rangle\langle\uparrow,\downarrow| + x_2|2\downarrow\rangle\langle 2\downarrow|, \qquad (1)\end{aligned}$$

where $x_0 = (\frac{1}{18} + \frac{5}{9}|\alpha|^2)$, $x_1 = \frac{5\sqrt{2}}{18}\alpha\beta^*$, $x_2 = \frac{1}{18} + \frac{5}{9}|\beta|^2$, and $|2\uparrow\equiv|\uparrow\uparrow\rangle$, similar for $|2\downarrow\rangle$, $|\uparrow,\downarrow\rangle = (|\uparrow\downarrow\rangle + |\downarrow\uparrow\rangle)/\sqrt{2}$ is the normalized symmetric state. This state is a mixed state so we cannot use available quantum cloning machines to obtain 3 copies. We propose the following 2 to 3 cloning machine to accomplish this task

$$\begin{aligned}U|2\uparrow\rangle\otimes R &= \frac{\sqrt{3}}{2}|3\uparrow\rangle\otimes R_\uparrow + \frac{1}{2}|2\uparrow,\downarrow\rangle\otimes R_\downarrow, \qquad (2)\\ U|2\downarrow\rangle\otimes R &= \frac{1}{2}|\uparrow,2\downarrow\rangle\otimes R_\uparrow + \frac{\sqrt{3}}{2}|\downarrow\rangle\otimes R_\downarrow, \qquad (3)\\ U|\uparrow,\downarrow\rangle\otimes R &= \frac{1}{\sqrt{2}}|2\uparrow,\downarrow\rangle\otimes R_\uparrow + \frac{1}{\sqrt{2}}|\uparrow,2\downarrow\rangle\otimes R_\downarrow (4)\end{aligned}$$

where state $|2\uparrow,\downarrow\rangle$ is a normalized symmetric state with 2 spin up and 1 spin down. We remark that the quantum cloning transformations (2,3) are the same as Gisin-Massar's original cloning machine where the input are identical pure states. The cloning transformation (4) is a new relation. In the quantum cloning processing with input $\rho^{(2)}_{red.}$ in (1), we first add blank state and the ancilla state, perform the quantum cloning transformations listed as (2,3,4), trace out the ancilla states and finally obtain 3 identical copies. The final reduced density operator of one single qubit has fidelity 79/108 compared with the initial available qubit $|\Psi\rangle$. Thus we show explicitly how to accomplish the simple but rather practical cloning task in quantum computation. This is a simple example to show that the cloning machine which can use any mixed states in symmetric space is very important in quantum computation.

The general quantum cloning machine: A much general problem is that part of the output state from one cloning machine is used for one quantum computation. The remaining quantum state need to be further cloned to create more copies but with a lower fidelity for another quantum computation. One can easily imagine more complicated problems where more than 2 cloning machines are needed. All of these problems can be solved if we can construct the cloning machines which can copy any mixed states in symmetric space.

With one simple but non-trivial example solved, we next present our general result. We assume $\{|i\rangle, i = 1,\cdots,d\}$ as orthonormal basis of d-level quantum system. We define $\vec{m} = \{m_1,\cdots,m_d\}$, and denote $|\vec{m}\rangle$ as completely symmetrical states with m_i states in $|i\rangle$, where $\sum_{i=1}^d m_i = M$, these are orthonormal basis of symmetric subspace of M d-level quantum system. Any quantum states in symmetric subspace is invariant under arbitrary permutations. We propose the following universal quantum cloning machine,

$$U|\vec{m}\rangle\otimes R = \sum_{\vec{k}} \alpha_{\vec{m}\vec{k}}|\vec{m}+\vec{k}\rangle\otimes R_{\vec{k}}, \qquad (5)$$

where $\sum_{\vec{k}}$ means summation over all possible parameters under the restriction $\sum_i k_i = N - M$, R represents blank states and ancilla states of the cloning machine before the cloning processing. $R_{\vec{k}}$ are the ancilla states of the output, we can simplely realize them by symmetric quantum state $|\vec{k}\rangle$. A simple example of this quantum cloning machine has already been presented in (2,3,4). Performing unitary transformation U, tracing out the ancilla states, we can obtain the output density operator $\rho^{(out)} = Tr_a U(\rho\otimes R)U^\dagger$. The amplitude of the output states take the form

$$\alpha_{\vec{m}\vec{k}} = \eta\sqrt{\prod_i \frac{(m_i+k_i)!}{m_i!k_i!}}, \qquad (6)$$

where $\eta = \sqrt{(N-M)!(M+d-1)!/(N+d-1)!}$ is the normalization factor. We know the BEM bound can be achieved for identical pure input states by Werner[8] and Keyl and Werner[9] (WKW) cloning machine. Here we show that BEM bound is the tight bound not only for pure states but also for arbitrary states in symmetric subspace. We can find the cloning transformation (5,6) realizes the WKW [8, 9] cloning machine.

References

[1] W.K.Wootters,W.H. Zurek,Nature 299,802(1982).

[2] M.A.Nielsen and I.L.Chuang, *Quantum computation and quantum information*, Cambridge University Press, 2000.

[3] N.Gisin, and S.Massar, Phys.Rev.Lett. 79, 2153 (1997).

[4] V.Buzek and M.Hillery, Phys.Rev.A 54, 1844 (1996).

[5] V.Buzek,H.Hillery, Phys.Rev.Lett.81, 5003(1998).

[6] N.J.Cerf, Phys.Rev.Lett.84,4497 (2000); J. Mod. Opt. 47, 187 (2000).

[7] D.Bruss, A.Ekert, C.Macchiavello, Phys. Rev.Lett. 81, 2598 (1998).

[8] R.Werner, Phys.Rev.A 58, 1827 (1998).

[9] M.Keyl,R.Werner, J.Math.Phys.40, 3283(1999).